

OpenID-Connect-PHP

github.com/jumbojett/OpenID-Connect-PHP

Scanned 24 September 2026 at 10:17 · Report generated 29 October 2026 · PHP · 738 stars

OVERALL ASSESSMENT

Low

Combined score 19 · 9 findings after filtering

Summary

This repository has a low vulnerability score of 19.0, which means there are some common coding mistakes that could be exploited if an attacker finds them. However, the code does not appear to contain malicious patterns or signs of intentional harm. The most serious issue is that SSL verification is disabled, allowing connections to be made without checking if the server is actually valid. Another significant risk is a specific YARA rule that detected downloading and executing remote files, which is extremely dangerous even though it was only found once. While there are other issues like missing dependency cooldowns and unsafe GitHub Actions steps, these do not change the overall picture of whether the code is safe to use right now.

Written by a language model running locally on the scanning machine, from the findings in this report. The risk levels above and below were decided by the scoring model, not by this summary.

Risk, by type

MalDet scores two different questions separately, because they call for different responses: code can be badly written without being hostile, and hostile code is not always badly written.

VULNERABILITY

Low (19)

Insecure coding an attacker could exploit. Usually mistakes, and usually fixable in place.

MALICIOUS PATTERN

Safe (0)

Signs the code may be trying to do harm: hidden payloads, credential access, persistence, exfiltration.

What each detector found

DETECTOR	LOOKS FOR	HIGH	MEDIUM	LOW	TOTAL
semgrep	Insecure coding patterns across many languages	1	7	0	8

DETECTOR	LOOKS FOR	HIGH	MEDIUM	LOW	TOTAL
yara	Signatures of malicious behaviour in source files	1	0	0	1

6 of 9 findings were rated more likely genuine than noise by the classifier.

Evidence

Identical findings are grouped, so a single rule firing many times takes one row. Ordered worst first. “Seen” is how many times that finding occurred.

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
HIGH	semgrep	SSL verification is disabled but should not be (currently CURLOPT_SSL_VERIFYPEER= false)	1	/src/OpenIDConnectClient.php:1427
HIGH	yara	YARA rule matched: detect_download_and_execute — Downloads a remote resource AND executes it - the actually dangerous combination, not just downloading alone	1	/src/OpenIDConnectClient.php
MEDIUM	semgrep	This Dependabot configuration does not set a cooldown period. Newly published packages can be malicious or unstable. Add a `cooldown` block with `default-days: 7` to each `package-ecosystem` entry under `updates` to wait 7 days before proposing updates to newly published package versions. Reference:	2	/.github/dependabot.yml:16
MEDIUM	semgrep	GitHub Actions step uses a mutable tag or branch reference. Tags and branch names can be silently repointed by the action owner, enabling supply-chain attacks — as seen in the trivy-action and kics-github-action compromises. Pin the reference to a full 40-character commit SHA instead, e.g. `uses: ac	3	/.github/workflows/build.yml:36
MEDIUM	semgrep	The `redirect()` method does not check its destination in any way. If you redirect to a URL provided by end-users, your application may be open to the unvalidated redirects security vulnerability. Consider using literal values or an allowlist to validate URLs.	2	/src/OpenIDConnectClient.php:795

How to read this report

- **This is a static scan.** The code was read, never executed. Behaviour that only appears at runtime is outside what any of these detectors can see.
- **Findings are not all equally real.** A classifier rates each finding on how likely it is to be genuine rather than noise, and that rating weights the scores. Measured against a hand-reviewed sample it reached precision 0.52 and recall 0.62 — useful for ranking, not a verdict on any single finding.
- **A high score is not proof of malice.** Security tools, penetration-testing frameworks and malware research repositories contain the same patterns as real malware by design. The two risk types above exist to keep that distinction visible.
- **Absence of findings is not proof of safety.** A detector that is not installed, or a language none of them parse, produces silence rather than a warning.
- **This scan is a snapshot.** The repository may have changed since 24 September 2026.